# Safeguarding Massive MIMO Aided HetNets Using Physical Layer Security

Yansha Deng*, Lifeng Wang†, Kai-Kit Wong†, Arumugam Nallanathan*, Maged Elkashlan‡,
and Sangarapillai Lambotharan §
*Department of Informatics, King's College London, London, UK
†Department of Electronic and Electrical Engineering, University College London, London, UK
‡School of Electronic Engineering and Computer Science, Queen Mary University of London, London, UK
§ Department of Electronic and Electrical Engineering, Loughborough University, Leicestershire, UK

***Abstract*—This paper exploits the potential of physical layer security in massive multiple-input multiple-output (MIMO) aided two-tier heterogeneous networks (HetNets). We focus on the downlink secure transmission in the presence of multiple eavesdroppers. We first address the impact of massive MIMO on the maximum receive power based user association. We then derive the tractable upper bound expressions for the secrecy outage probability of a HetNets user. We show that the implementation of massive MIMO significantly improves the secrecy performance, which indicates that physical layer security could be a promising solution for safeguarding massive MIMO HetNets. Furthermore, we show that the secrecy outage probability of HetNets user first degrades and then improves with increasing the density of PBSs.**

## I. Introduction

Security and privacy in 5G networks is of paramount importance [1], [2]. Physical layer security has recently attracted much attention as a potential security solution at the physical layer [3]. Such security technique exploits propagation randomness to establish secret and avoids using ciphering keys. The FP7 Europe research project PHYLAWS [4] focuses on the realistic implantation of physical layer security in the existing and future wireless networks.

Research efforts on the physical layer security have been made by considering different aspects, such as antenna selection [5], cooperative jamming [6], and artificial noise [7], etc. In [8], matched filter precoding and artificial noise generation was designed to secure downlink transmission in a multicell massive multiple-input multiple-output (MIMO) system in the presence of an eavesdropper. In [9], physical layer security has been investigated in a two-tier downlink HetNets, where the cooperative femtocells help macrocell achieve the optimal secrecy transmit beamforming.

In 5G, massive multiple-input multiple-output (MIMO) and heterogeneous networks (HetNets) are two key enablers. Physical layer security in massive MIMO enabled HetNets has not been conducted yet and is in its infancy. We believe that massive MIMO enabled HetNets is a new highly rewarding candidate for physical layer security due to the following factors:

- **Base station densities**. In HetNets, different tiers have different base station densities, and small cells are deployed in a large scale to improve the spectrum efficiency. As such, the distance between the user and its serving base station is shorter, which in turn decreases the risk of information leakage.
- **Large antenna arrays**. Base station with large antenna array provides large array gain for its legitimate user. As such, the transmit power level can be cut, and the received signal power at the eavesdropper is correspondingly reduced, due to the fact that the eavesdropper cannot obtain the array gain.
- **Time division duplex**. Massive MIMO is recommended to be applied in time division duplex (TDD) system, to save the pilot resources. In the TDD mode, base station estimates the uplink channel via uplink pilot signals from user, and obtains the downlink channel state information (CSI) based on the channel reciprocity, which means that there is no channel training in the downlink. As such, eavesdropper cannot easily estimate the eavesdropper's channel during the downlink transmission.

Motivated by the above, this paper considers physical layer security in the downlink $K$-tier HetNets with massive MIMO, which to the best of our knowledge, has not been studied yet. Each macrocell base station (MBS) is equipped with large antenna arrays and uses linear zero-forcing beamforming (ZFBF) to communicate with dozens of single antenna users over the same time and frequency band. Each picocell base station (PBS) equipped with a single antenna serves one single antenna user for each transmission. We adopt a stochastic geometry approach to model the different tiers, where the locations of MBSs, PBSs and eavesdroppers are modelled following independent homogeneous Poisson point processes. We first address the impact of massive MIMO on the maximum receive power based user association. We then derive the upper bound for the secrecy outage probability of a HetNets user, to show the benefits of massive MIMO. Our results confirms that using massive MIMO can significantly enhance the secrecy outage probability of the macrocell user. Furthermore, the secrecy outage probability of the HetNets user first increases and then decreases with increasing the density of PBSs.

978-1-4673-7687-7/15/$31.00 ©2015 IEEE

## II. System Model

In the TDD two-tier HetNets consisting of macrocells and picocells, downlink transmission is considered in the presence of multiple eavesdroppers. Without loss of generality, we assume that the first tier represents the class of MBSs. The MBSs are located following a homogeneous Poisson point process (HPPP) $\Phi_\mathrm{M}$ with density $\lambda_\mathrm{M}$, while the PBSs are located following an independent HPPP $\Phi_\mathrm{P}$ with density $\lambda_\mathrm{P}$. The eavesdroppers are located following an independent HPPP $\Phi_\mathrm{E}$ with density $\lambda_\mathrm{E}$.

Massive MIMO is adopted in the macrocells [10], where each $N$-antenna MBS simultaneously communicates with $S$ users $(N \gg S \geq 1)$, while each PBS and user are single-antenna nodes. Each MBS uses ZFBF to transmit $S$ data streams with equal power assignment, such that users that act as potential malicious eavesdropper can only receive its information signals. We consider the perfect downlink CSI and the universal frequency reuse that all the tiers share the same bandwidth. All the channels undergo independent and identically distributed (i.i.d.) quasi-static Rayleigh fading.

### A. User Association

We consider user association based on the maximum received power, where a user is associated with the BS that provides the maximum average received power. The average received power at a user that is connected with the MBS $\ell$ $(\ell \in \Phi_\mathrm{M})$ is expressed as

$$P_{r,\mathrm{M}} = G_a \frac{P_\mathrm{M}}{S} L\left(|X_{\ell,\mathrm{M}}|\right), \qquad (1)$$

where $G_a$ is the array gain, $P_\mathrm{M}$ is the MBS's transmit power, $L\left(|X_{\ell,\mathrm{M}}|\right) = \beta |X_{\ell,\mathrm{M}}|^{-\alpha_\mathrm{M}}$ is the path loss function, $\beta$ is the frequency dependent constant value, $|X_{\ell,\mathrm{M}}|$ is the distance, and $\alpha_1$ is the path loss exponent. The array gain $G_a$ of ZFBF transmission is $N - S + 1$ [11].

In the picocell, the long-term average received power at a user that is connected with the PBS $j$ $(j \in \Phi_\mathrm{P})$ is expressed as

$$P_{r,\mathrm{P}} = P_\mathrm{P} L\left(|X_{j,\mathrm{P}}|\right), \qquad (2)$$

where $P_\mathrm{P}$ is the PBS's transmit power and $L\left(|X_{j,P}|\right) = \beta(|X_{j,\mathrm{P}}|)^{-\alpha_2}$ with distance $|X_{j,\mathrm{P}}|$ and path loss exponent $\alpha_2$.

### B. Channel Model

All the channels undergo the independent and identically distributed (i.i.d.) quasi-static Rayleigh fading. We assume that a typical user is located at the origin $o$. The receive signal-to-interference-plus-noise ratio (SINR) of a typical user at a random distance $|X_{o,\mathrm{M}}|$ from its associated MBS is given by

$$\mathrm{SINR}_\mathrm{M} = \frac{\frac{P_\mathrm{M}}{S} h_{o,\mathrm{M}} L\left(|X_{o,\mathrm{M}}|\right)}{I_1 + \delta^2}, \qquad (3)$$

where $I_1 = I_{\mathrm{M},1} + I_{\mathrm{S},1}$, $I_{\mathrm{S},1} = \sum_{j\in\Phi_\mathrm{P}} P_\mathrm{P} h_{j,\mathrm{P}} L\left(|X_{j,\mathrm{P}}|\right)$, $I_{\mathrm{M},1} = \sum_{\ell\in\Phi_\mathrm{M}\backslash B_{o,\mathrm{M}}} \frac{P_\mathrm{M}}{S} h_{\ell,\mathrm{M}} L\left(|X_{\ell,\mathrm{M}}|\right)$, $h_{o,\mathrm{M}} \sim \Gamma\left(N - S + 1, 1\right)$ is the small-scale fading channel power gain between the typical user and its associated MBS [11], $h_{j,\mathrm{P}} \sim \exp(1)$ and $|X_{j,\mathrm{P}}|$ are the small-scale fading interfering channel power gain and distance between the typical user and BS $j$ in the picocell, respectively, $h_{\ell,\mathrm{M}} \sim \Gamma\left(S, 1\right)$ and $|X_{\ell,\mathrm{M}}|$ are the equivalent small-scale fading interfering channel power gain and distance between the typical user and MBS $\ell \in \Phi_\mathrm{M}\backslash B_{o,\mathrm{M}}$ (except the serving BS $B_{o,\mathrm{M}}$), respectively, and $\delta^2$ is the noise power.

The SINR of a typical user at a random distance $|X_{o,\mathrm{P}}|$ from its associated PBS $B_{o,\mathrm{P}}$ is given by

$$\mathrm{SINR}_\mathrm{P} = \frac{P_\mathrm{P} g_{o,\mathrm{P}} L\left(|X_{o,\mathrm{P}}|\right)}{I_2 + \delta^2}, \qquad (4)$$

where $I_2 = I_{\mathrm{M},2} + I_{\mathrm{S},2}$, $I_{\mathrm{M},2} = \sum_{\ell\in\Phi_\mathrm{M}} \frac{P_\mathrm{M}}{S} g_{\ell,\mathrm{M}} L\left(|X_{\ell,\mathrm{M}}|\right)$, $I_{\mathrm{S},2} = \sum_{j\in\Phi_\mathrm{P}\backslash B_{o,\mathrm{P}}} P_\mathrm{P} g_{j,\mathrm{P}} L\left(|X_{j,\mathrm{P}}|\right)$, $g_{o,\mathrm{P}} \sim \exp(1)$ is the small-scale fading channel power gain between the typical user and its serving BS, $g_{\ell,\mathrm{M}} \sim \Gamma\left(S, 1\right)$ and $|X_{\ell,\mathrm{M}}|$ are the equivalent small-scale fading interfering channel power gain and distance between the typical user and MBS $\ell$, respectively, and $g_{j,\mathrm{P}}$ and $|X_{j,\mathrm{P}}|$ are the small-scale fading interfering channel power gain and distance between the typical user and BS $j \in \Phi_\mathrm{P}\backslash B_{o,\mathrm{P}}$, respectively, and $g_{j,\mathrm{P}} \sim \exp(1)$.

We consider the non-colluding and passive eavesdropping that each eavesdropper intercepts the signal independently without any attacks. In this case, we only need to focus on the most malicious eavesdropper that has the largest receive SINR. When the MBS transmits the information messages to its intended user, the receive SINR at the most malicious eavesdropper is given by

$$\mathrm{SINR}^\mathrm{M}_{e^*} = \max_{e\in\Phi_\mathrm{E}} \left\{ \frac{\frac{P_\mathrm{M}}{S} h_{o,e} L\left(|X_{o,e}|\right)}{I_A + I_{\mathrm{M},e} + I_{\mathrm{S},e} + \delta^2} \right\}, \qquad (5)$$

where $h_{o,e} \sim \exp(1)$ and $|X_{o,e}|$ are the equivalent small-scale fading channel power gain and distance between the eavesdropper and its targeted BS, respectively, $I_A = \frac{P_\mathrm{M}}{S} h_e L\left(|X_{o,e}|\right)$ with $h_e \sim \Gamma\left(S - 1, 1\right)$ is the intra-cell interference in the macro cell, $I_{\mathrm{M},e} = \sum_{\ell\in\Phi_\mathrm{M}\backslash o} \frac{P_\mathrm{M}}{S} h_{\ell,e} L\left(|X_{\ell,e}|\right)$, $h_{\ell,e} \sim \Gamma\left(S, 1\right)$ and $|X_{\ell,e}|$ are the equivalent small-scale fading interfering channel power gain and distance between the eavesdropper and MBS $\ell$, respectively, $I_{\mathrm{S},e} = \sum_{j\in\Phi_\mathrm{P}} P_\mathrm{P} h_{j,\mathrm{P},e} L\left(|X_{j,\mathrm{P},e}|\right)$, $h_{j,\mathrm{P},e} \sim \exp(1)$ and $|X_{j,\mathrm{P},e}|$ are the small-scale fading interfering channel power gain and distance between the eavesdropper and BS $j$ in the picocell, respectively. Similarly. when the PBS transmits the information messages to its intended user, the receive SINR at the most malicious eavesdropper is given by

$$\mathrm{SINR}^\mathrm{P}_{e^*} = \max_{e\in\Phi_\mathrm{E}} \left\{ \frac{P_\mathrm{P} g_{o,e} L\left(|X_{o,e}|\right)}{I_{\mathrm{M,P},e} + I_{\mathrm{S,P},e} + \delta^2} \right\}, \qquad (6)$$

where $g_{o,e} \sim \exp(1)$ and $|X_{o,e}|$ are the equivalent small-scale fading channel power gain and distance between the eavesdropper and its targeted BS, respectively, $I_{\mathrm{M,P},e} = \sum_{\ell\in\Phi_\mathrm{M}} \frac{P_\mathrm{M}}{S} g_{\ell,e} L\left(|X_{\ell,e}|\right)$, $g_{\ell,e} \sim \Gamma\left(S, 1\right)$ and $|X_{\ell,e}|$ are the equivalent small-scale fading interfering channel power gain and distance between the eavesdropper and MBS $\ell$, respectively, $I_{\mathrm{S,P},e} = \sum_{j\in\Phi_\mathrm{P}\backslash o} P_\mathrm{P} g_{j,\mathrm{P},e} L\left(|X_{j,\mathrm{P},e}|\right)$, $g_{j,\mathrm{P},e} \sim \exp(1)$

and $|X_{j,\mathrm{P},e}|$ are the small-scale fading interfering channel power gain and distance between the eavesdropper and BS $j$ in the picocell, respectively.

## III. Secrecy Performance

In an effort to assess the secrecy outage probability of a HetNets user, we first characterize the impact of massive MIMO on the cell association probability.

### A. User Association Probability

We first derive the PDF of the distance between a typical user and its serving base station in the following two lemmas.

**Lemma 1.** The PDF of the distance $|X_{o,\mathrm{M}}|$ between a typical user and its serving MBS $B_{o,\mathrm{M}}$ is given by

$$\begin{aligned} f_{|X_{o,\mathrm{M}}|}(x) =& \frac{2\pi\lambda_{\mathrm{M}}}{\mathcal{A}_{\mathrm{M}}} x \exp\Bigg\{ -\pi\lambda_{\mathrm{M}} x^2 \\ & -\pi\lambda_{\mathrm{P}} \left( \frac{SP_{\mathrm{P}}}{(N-S+1)P_{\mathrm{M}}} \right)^{2/\alpha_2} x^{2\alpha_1/\alpha_2} \Bigg\}. \end{aligned} \tag{7}$$

In (7), $\mathcal{A}_{\mathrm{M}}$ is the probability that a typical user is associated with the MBS

$$\begin{aligned} \mathcal{A}_{\mathrm{M}} =& 2\pi\lambda_{\mathrm{M}} \int_0^\infty r \exp\Bigg\{ -\pi\lambda_{\mathrm{M}} r^2 \\ & -\pi\lambda_{\mathrm{P}} \left( \frac{SP_{\mathrm{P}}}{(N-S+1)P_{\mathrm{M}}} \right)^{2/\alpha_2} r^{2\alpha_1/\alpha_2} \Bigg\} dr. \end{aligned} \tag{8}$$

**Lemma 2.** *The PDF of the distance $|X_{o,k}|$ between a typical user and its serving PBS in $\mathrm{B}_{o,\mathrm{P}}$ is given by*

$$\begin{aligned} f_{|X_{o,\mathrm{P}}|}(x) =& \frac{2\pi\lambda_{\mathrm{P}}}{\mathcal{A}_{\mathrm{P}}} x \exp\Bigg\{ -\pi\lambda_{\mathrm{P}} x^2 \\ & -\pi\lambda_{\mathrm{M}} \left( \frac{P_{\mathrm{M}}(N-S+1)}{P_{\mathrm{P}}S} \right) x^{2\alpha_2/\alpha_1} \Bigg\}. \end{aligned} \tag{9}$$

Here, $\mathcal{A}_{\mathrm{P}}$ is the probability that a typical user is associated with the PBS, which is given by

$$\begin{aligned} \mathcal{A}_{\mathrm{P}} =& 2\pi\lambda_{\mathrm{P}} \int_0^\infty r \exp\Bigg\{ -\pi\lambda_{\mathrm{P}} r^2 \\ & -\pi\lambda_{\mathrm{M}} \left( \frac{P_{\mathrm{M}}(N-S+1)}{P_{\mathrm{P}}S} \right) r^{2\alpha_2/\alpha_1} \Bigg\} dr. \end{aligned} \tag{10}$$

Note that Lemma 1 and Lemma 2 can be derived following the approach in [12].

### B. Achievable Ergodic Rate

In this subsection, we derive the achievable ergodic rate of the macrocell user and the picocell user.

**Lemma 3.** *For a typical user at a random distance $|X_{o,\mathrm{M}}|$ from its associated MBS, the lower bound on the achievable ergodic rate of the typical macrocell user is derived as*

$$R_{\mathrm{M}}^{L} = \log_2\left( 1 + \frac{P_{\mathrm{M}}}{S}(N-S+1)\beta \left( \frac{2\pi\lambda_{\mathrm{M}}}{\mathcal{A}_{\mathrm{M}}}\Delta \right)^{-1} \right), \tag{11}$$

*where*

$$\begin{aligned} \Delta = \int_0^\infty & \left( \frac{2\pi\lambda_{\mathrm{M}} P_{\mathrm{M}} \beta x^{2-\alpha_1}}{\alpha_1 - 2} + \frac{2\pi\lambda_{\mathrm{P}} P_{\mathrm{P}} \beta \left( D_{\mathrm{P}}^{\mathrm{M}}(x) \right)^{2-\alpha_2}}{\alpha_2 - 2} + \delta^2 \right) \\ & \exp\left\{ -\pi\lambda_{\mathrm{M}} x^2 - \pi\lambda_{\mathrm{P}} \left( D_{\mathrm{P}}^{\mathrm{M}}(x) \right)^2 \right\} x^{\alpha_1+1} dx. \end{aligned} \tag{12}$$

*In* (12), $D_{\mathrm{P}}^{\mathrm{M}}(x) = \left( \frac{SP_{\mathrm{P}}}{(N-S+1)P_{\mathrm{M}}} \right)^{1/\alpha_2} x^{\alpha_1/\alpha_2}$ *is the minimum distance between the interfering picocell BS and the typical marcocell user.*

*Proof.* The achievable ergodic rate of macrocell user is lower bounded by

$$\mathbb{E}\{\log_2(1+\mathrm{SINR}_{\mathrm{M}})\} \geq R_{\mathrm{M}}^{L} = \log_2\left( 1 + \left( E\left\{ \mathrm{SINR_M}^{-1} \right\} \right)^{-1} \right), \tag{13}$$

where

$$\begin{aligned} \mathbb{E}\left\{ \mathrm{SINR_M}^{-1} \right\} =& \left( \frac{P_{\mathrm{M}}}{S}(N-S+1)\beta \right)^{-1} \\ & \int_0^\infty (E\{I_2\} + \delta^2) x^{\alpha_1} f_{|X_{o,\mathrm{M}}|}(x)\, dx. \end{aligned} \tag{14}$$

In (14), $f_{|X_{o,\mathrm{M}}|}(x)$ is given in (7). Using the Campbell's theorem, the expectation of the aggregate interference from the MBSs and the PBSs is derived as

$$\mathbb{E}\{I_2\} = \frac{2\pi\lambda_M P_{\mathrm{M}} \beta x^{2-\alpha_1}}{\alpha_1 - 2} + \frac{2\pi\lambda_{\mathrm{P}} P_{\mathrm{P}} \beta \left( D_{\mathrm{P}}^{\mathrm{M}}(x) \right)^{2-\alpha_2}}{\alpha_2 - 2}. \tag{15}$$

□

**Lemma 4.** *For a typical user at a random distance $|X_{o,\mathrm{P}}|$ from its associated PBS, the achievable ergodic rate of the typical picocell user is derived as*

$$R_{\mathrm{P}} = \mathbb{E}\{\log_2(1+\mathrm{SINR}_{\mathrm{P}})\} = \frac{1}{\ln 2} \int_0^\infty \frac{1 - \mathbb{F}_{\mathrm{SINR_P}}(\gamma)}{1+\gamma} d\gamma, \tag{16}$$

*where*

$$\begin{aligned} \mathbb{F}_{\mathrm{SINR_P}}(\gamma) = 1 - \frac{2\pi\lambda_{\mathrm{P}}}{\mathcal{A}_{\mathrm{P}}} \int_0^\infty & \exp\Bigg\{ -2\pi\lambda_{\mathrm{M}} \Phi_3(x) - 2\pi\lambda_{\mathrm{P}} \\ & \frac{x^2\gamma}{\alpha_2 - 2} {}_2F_1\left( 1, 1 - \frac{-2}{\alpha_2}, 2 - \frac{2}{\alpha_2}, -\gamma \right) - \frac{x^{\alpha_2}\gamma\delta^2}{P_{\mathrm{P}}\beta} \\ & -\pi\lambda_{\mathrm{P}} x^2 - \pi\lambda_{\mathrm{M}} \left( \frac{P_{\mathrm{M}}(N-S+1)x^{\alpha_2}}{P_{\mathrm{P}}S} \right)^{2/\alpha_1} \Bigg\} x dx. \end{aligned} \tag{17}$$

*In* (17)*, we have*

$$\begin{aligned} \Phi_3(x) =& {}_2F_1\left[ 1 - 2/\alpha_1, S, 2 - 2/\alpha_1, -\frac{\gamma \mathrm{P_M} x^{\alpha_2}}{SP_{\mathrm{P}} \left( D_{\mathrm{M}}^{\mathrm{P}}(x) \right)^{\alpha_1}} \right] \\ & \frac{\gamma P_{\mathrm{M}} x^{\alpha_2} \left( D_{\mathrm{M}}^{P}(x) \right)^{2-\alpha_1}}{SP_{\mathrm{P}}(\alpha_1 - 2)} + \sum_{k=2}^{S} \binom{S}{k} \frac{1}{\alpha_1} \left( -\frac{\gamma P_{\mathrm{M}} x^{\alpha_2}}{SP_{\mathrm{P}}} \right)^{2/\alpha_1} \\ & B\left( -\frac{\gamma P_{\mathrm{M}} x^{\alpha_2}}{SP_{\mathrm{P}} \left( D_{\mathrm{M}}^{\mathrm{P}}(x) \right)^{\alpha_1}}; k - 2/\alpha_1, 1 - S \right), \end{aligned} \tag{18}$$

*where* $D_{\mathrm{M}}^{\mathrm{P}}(x) = \left(\frac{(N-S+1)P_{\mathrm{M}}}{SP_{\mathrm{P}}}\right)^{1/\alpha_1} x^{\alpha_2/\alpha_1}$ *is the minimum distance between the interfering macrocell BS and the typical picocell user,* $B(\cdot;\cdot,\cdot)$*is the incomplete beta function [13, 8.391], and* ${}_2F_1[\cdot,\cdot,\cdot]$ *is the Gauss hypergeometric function [13, 9.142].*

*Proof.* The CDF of $\mathrm{SINR_P}$ is expressed as

$$\begin{aligned}\mathbb{F}_{\mathrm{SINR_P}}(\gamma) &= \int_0^\infty \Pr\left[g_{o,P} \le \frac{\gamma\left(I_2+\delta^2\right)}{P_{\mathrm{P}}\beta x^{-\alpha_2}}\right] f_{|X_{o,P}|}(x)\,dx \\ &= 1-\int_0^\infty \exp\left\{-\frac{\gamma\delta^2 x^{\alpha_2}}{P_{\mathrm{P}}\beta}\right\}\mathcal{L}_{I_2}\left(\frac{\gamma x^{\alpha_2}}{P_{\mathrm{P}}P\beta}\right) f_{|X_{o,P}|}(x)\,dx\end{aligned} \tag{19}$$

To solve the laplace transform of the aggregate interference from macrocell BSs and picocell BS, we first utilize $\mathcal{L}_{I_2}\left(\frac{\gamma x^{\alpha_2}}{P_{\mathrm{P}}\beta}\right) = \mathcal{L}_{I_{\mathrm{M},2}}\left(\frac{\gamma x^{\alpha_2}}{P_{\mathrm{P}}\beta}\right)\mathcal{L}_{I_{\mathrm{P},2}}\left(\frac{\gamma x^{\alpha_2}}{P_{\mathrm{P}}\beta}\right)$. The laplace transform of $I_{\mathrm{M},2}$ is given by

$$\begin{aligned}&\mathcal{L}_{I_{\mathrm{M},2}}(s) \\ &= \mathbb{E}_{I_{\mathrm{M},2}}\left\{\prod_{\ell\in\Phi_{\mathrm{M}}}\mathbb{E}_g\left\{\exp\left(-s\frac{P_{\mathrm{M}}g_{\ell,\mathrm{M}}\beta|X_{\ell,\mathrm{M}}|^{-\alpha_1}}{S}\right)\right\}\right\} \\ &\overset{(a)}{=} \exp\left\{-2\pi\lambda_{\mathrm{M}}\int_{D_{\mathrm{M}}^{\mathrm{P}}(x)}^\infty\left(1-\left(1+s\frac{P_{\mathrm{M}}\beta y^{-\alpha_1}}{S}\right)^{-S}\right)ydy\right\},\end{aligned} \tag{20}$$

where $(a)$ follows from probability generating functional (PGFL) of PPP [14] and the Cartesian to polar coordinates transformation. The Laplace transform of $I_{\mathrm{P},2}$ is given by

$$\begin{aligned}&\mathcal{L}_{I_{\mathrm{P},2}}(s) \\ &= \mathbb{E}_{I_{\mathrm{P},2}}\left\{\prod_{j\in\Phi_{\mathrm{P}}\backslash B_{o,\mathrm{P}}}E_g\left\{\exp\left(-sP_{\mathrm{P}}g_{j,\mathrm{P}}\beta|X_{j,\mathrm{P}}|^{-\alpha_2}\right)\right\}\right\} \\ &= \exp\left(-2\pi\lambda_{\mathrm{P}}\int_x^\infty\left(1-\left(1+sP_{\mathrm{P}}\beta r^{-\alpha_2}\right)^{-1}\right)rdr\right).\end{aligned} \tag{21}$$

Substituting (20) and (21) into (19), we finally derive (17). □

### C. Secrecy Outage Probability

Secrecy outage probability is the principle performance metric in the passive eavesdropping scenario. The secrecy outage is declared when the instantaneous secrecy rate is less than the targeted secrecy rate $R_s$ [15].

**Theorem 1.** *For a typical user associated with the MBS, the upper bound on the secrecy outage probability of this typical user is given by*

$$\begin{aligned}P_{out}^{\mathrm{M}}(R_s) &= \Pr\left\{R_{\mathrm{M}}-\log_2\left(1+\mathrm{SINR}_{e*}^{\mathrm{M}}\right)\le R_s\right\} \\ &= 1-\mathbb{F}_{\mathrm{SINR}_{e*}^{\mathrm{M}}}\left(2^{(R_{\mathrm{M}}-R_s)}-1\right),\end{aligned} \tag{22}$$

*where* $R_{\mathrm{M}}$ *is the lower bound of the ergodic rate of the macrocell user in* (13), $R_s$ *is the targeted secrecy rate, and the CDF of the receive SINR at the most malicious eavesdropper is derived as*

$$\begin{aligned}&\mathbb{F}_{\mathrm{SINR}_{e*}^{\mathrm{M}}}(\gamma) = \exp\left\{-2\pi\lambda_{\mathrm{E}}\int_0^\infty \exp\left\{-\gamma S\delta^2 x^{\alpha_1}(\beta P_{\mathrm{M}})^{-1}\right.\right. \\ &-2\pi\lambda_{\mathrm{M}}\sum_{k=1}^{S}\binom{S}{k}\frac{(\gamma x^{\alpha_1})^{2/\alpha_1}\Gamma(k-2/\alpha_1)\Gamma(-k+2/\alpha_1+S)}{\alpha_1\Gamma(S)} \\ &\left.-\frac{2\pi^2\lambda_{\mathrm{P}}}{\alpha_2}\left(\gamma Sx^{\alpha_1}P_{\mathrm{P}}(P_{\mathrm{M}})^{-1}\right)^{2/\alpha_2}Csc\left[2\pi/\alpha_2\right]\right\} \\ &\left.(\gamma+1)^{-(S-1)}xdx\right\}.\end{aligned} \tag{23}$$

**Theorem 2.** *For a typical user associated with the PBS, the secrecy outage probability of this typical user is derived as*

$$\begin{aligned}P_{out}^{\mathrm{P}}(R_s) &= \Pr\left\{R_{\mathrm{P}}-\log_2\left(1+\mathrm{SINR}_{e*}^{\mathrm{P}}\right)\le R_s\right\} \\ &= 1-\mathbb{F}_{\mathrm{SINR}_{e*}^{\mathrm{P}}}\left(2^{(R_{\mathrm{P}}-R_s)}-1\right),\end{aligned} \tag{24}$$

*where* $R_{\mathrm{P}}$ *is the achievable ergodic rate of the picocell user in* (16), *and the CDF of the receive SINR at the most malicious eavesdropper is given by*

$$\begin{aligned}&\mathbb{F}_{\mathrm{SINR}_{e*}^{\mathrm{P}}}(\gamma) = \exp\left\{-2\pi\lambda_{\mathrm{E}}\int_0^\infty \exp\left\{-\gamma\delta^2 x^{\alpha_2}(\beta P_{\mathrm{P}})^{-1}\right.\right. \\ &-2\pi\lambda_M\sum_{k=1}^{S}\binom{S}{k}\left(\frac{\gamma P_{\mathrm{M}}}{P_{\mathrm{P}}S}\right)^{2/\alpha_1}\frac{\Gamma(-k+2/\alpha_1+S)\Gamma(k-2/\alpha_1)}{\alpha_1\Gamma(S)} \\ &\left.\left.x^{2\alpha_2/\alpha_1}-\frac{2\pi^2\lambda_{\mathrm{P}}}{\alpha_2}\gamma^{2/\alpha_2}Csc\left[2\pi/\alpha_2\right]x^2\right\}xdx\right\}.\end{aligned} \tag{25}$$

The results in Theorem 1 and Theorem 2 can be derived following the similar approach in the proof for Lemma 4.

The secrecy outage probability of the HetNets user is given by

$$P_{out}(R_s) = P_{out}^{\mathrm{M}}(R_s)\mathcal{A}_{\mathrm{M}} + P_{out}^{\mathrm{P}}(R_s)\mathcal{A}_{\mathrm{P}}, \tag{26}$$

where $\mathcal{A}_{\mathrm{M}}$ and $\mathcal{A}_{\mathrm{P}}$ are the user cell association probability in the macrocell and the picocell, which are derived in (8) and (10).

## IV. Numerical Examples

In this section, we evaluate the achievable ergodic rate and the secrecy outage probability of the considered massive MIMO HetNets based on the analytical results derived in Section III and Monte Carlo simulation. We consider a downlink HetNets in a circular region with radius 100m. In all simulations, we assume that the network operates at the carrier frequency 1GHz, the bandwidth is 10MHz, the transmit power of the MBS is $P_{\mathrm{M}} = 46$ dBm, the transmit power of the PBS is $P_{\mathrm{P}} = 37$ dBm, the path loss exponent of macrocell is $\alpha_1 = 3.5$, the path loss exponent of picocell is $\alpha_2 = 4$, the density of MBSs is $\lambda_{\mathrm{M}} = 10^{-3}$, the density of eavesdroppers is $\lambda_{\mathrm{E}} = 10^{-1}$, the users simultaneously served by each MBS is $S = 10$, and the thermal noise is $\sigma^2 = -90$ dBm. Both figures show that the analytical plots have a good match with the simulation plots.

Fig. 1 plots the ergodic rate of the marcocell user and the picocell user versus the number of antennas at each MBS $N$

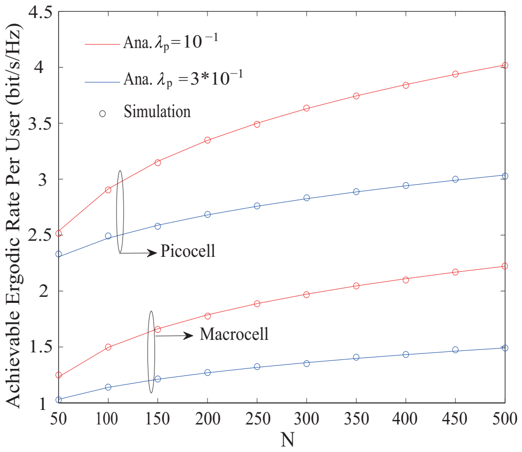

Fig. 1. Achievable ergodic rate versus the number of antennas at each MBS

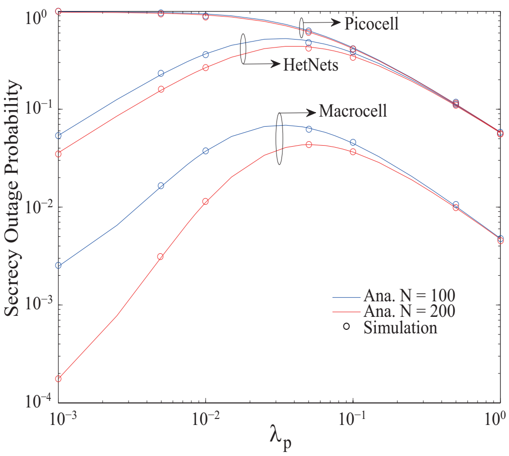

Fig. 2. Secrecy outage probability versus the density of PBSs

using (11) and (16). It is shown that the achievable ergodic rate improves with increasing $N$, due to the large array gain. This indicates that massive MIMO MBS carries more data traffic. Interestingly, increasing the density of PBSs, the achievable ergodic rates of the marcocell user and the picocell user degrade. This is due to the dominant impact of increased intercell interference brought by the PBSs.

Fig. 2 plots the achievable secrecy outage probability versus the density of the PBSs. We set the number of antennas at each MBS as $N = 200$, and define the targeted secrecy rate at the marcocell user as $R_s = \rho R_{\rm M}$, and the targeted secrecy rate at the picocell user as $R_s = \rho R_{\rm P}$. It is assumed that $\rho = 0.5$. We see that the secrecy outage probability of the picocell user decreases with increasing $\lambda_{\rm P}$, due to the fact that more interference results in lowering ${\rm SINR_P}$ in (4).

More importantly, the secrecy outage probability of macrocell user first degrades then improves with increasing $\lambda_{\rm P}$. The reason is that: 1) Increasing $\lambda_{\rm P}$ increases the interference from PBSs, thus greatly degrades ${\rm SINR_M}$ in (3); 2) For very large density of PBSs, the interference from the interfering PBSs dominates ${\rm SINR}_{e^*}^{\rm M}$ in (5). Increasing $\lambda_{\rm P}$ greatly decreases the distance between the interfering PBSs and the typical eavesdropper, and thus largely decreases ${\rm SINR}_{e^*}^{\rm M}$.

## V. Conclusion

In this paper, we took into account the physical layer security for the downlink massive MIMO HetNets with linear zero-forcing beamforming (ZFBF), where the non-colluding malicious eavesdroppers intercept the downlink user's transmission. Our work demonstrated the importance of BS deployment density and massive MIMO design on safeguarding the secure downlink transmission in HetNets.

## VI. Acknowledgement

This work was supported by the UK Engineering and Physical Sciences Research Council (EPSRC) with Grant No. EP/M016145/1.

## References

[1] 5GPPP, 5G Vision. [Online]. Available: http://5g-ppp.eu/wp-content/uploads/2015/02/5G-Vision-Brochure-v1.pdf

[2] N. Yang, L. Wang, G. Geraci, M. Elkashlan, J. Yuan, and M. Di Renzo, "Safeguarding 5G wireless communication networks using physical layer security," *IEEE Commun. Mag.*, vol. 53, no. 4, pp. 20–27, Apr. 2015.

[3] A. D. Wyner, "The wire-tap channel," *Bell Syst. Technol. J.*, vol. 54, no. 8, pp. 1355–1387, Oct. 1975.

[4] FP7 European Project, PHYsical LAyer Wireless Security (PHYLAWS). [Online]. Available: http://www.phylaws-ict.org/

[5] L. Wang, M. Elkashlan, J. Huang, R. Schober, and R. K. Mallik, "Secure transmission with antenna selection in MIMO nakagami-$m$ fading channels," *IEEE Trans. Wireless Commun.*, vol. 13, no. 11, pp. 6054–6067, Nov. 2014.

[6] G. Zheng, L.-C. Choo, and K.-K. Wong, "Optimal cooperative jamming to enhance physical layer security using relays," *IEEE Trans. Signal Process.*, vol. 59, no. 3, pp. 1317–1322, Mar. 2011.

[7] Y. Deng, L. Wang, S. A. R. Zaidi, J. Yuan, and M. Elkashlan, "On the security of large scale spectrum sharing networks," in *Proc. IEEE ICC*, 2015, pp. 1–6.

[8] J. Zhu, R. Schober, and V. Bhargava, "Secure transmission in multicell massive MIMO systems," *IEEE Trans. Wireless Commun.*, vol. 13, no. 9, pp. 4766–4781, 2014.

[9] T. Lv, H. Gao, and S. Yang,"Secrecy transmit beamforming for heterogeneous networks," *accepted by IEEE J. Sel. Areas Commun.*, pp. 1-17, 2015.

[10] V. Jungnickel, K. Manolakis, W. Zirwas, B. Panzner, V. Braun, M. Lossow, M. Sternad, R. Apelfrojd, and T. Svensson, "The role of small cells, coordinated multipoint, and massive MIMO in 5G," *IEEE Commun. Mag.*, vol. 52, no. 5, pp. 44–51, May 2014.

[11] K. Hosseini, W. Yu, and R. S. Adve, "Large-scale MIMO versus network MIMO for multicell interference mitigation," *IEEE J. Sel. Areas Commun.*, vol. 8, no. 5, pp. 930–941, Oct. 2014.

[12] H.-S. Jo, Y. J. Sang, P. Xia, and J. Andrews, "Heterogeneous cellular networks with flexible cell association: A comprehensive downlink sinr analysis," *IEEE Trans. Wireless Commun.*, vol. 11, no. 10, pp. 3484–3495, October 2012.

[13] I. S. Gradshteyn and I. M. Ryzhik, *Table of Integrals, Series and Products*, 7th ed. San Diego, C.A.: Academic Press, 2007.

[14] D. Stoyan, W. Kendall, and J. Mecke, "Stochastic geometry and its applications," *Wiley New York*, vol. 2, 1987.

[15] J. Zhu, R. Schober, and V. K. Bhargava, "Secure transmission in multicell massive mimo systems," *IEEE Trans. Wireless Commun.*, vol. 13, no. 9, pp. 4766–4781, Sept 2014.